Spring 2007
Industry Study

Final Report
Information and Communications Technology Industry

The Industrial College of the Armed Forces
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
2007 Information and Communications Technology Industry	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Industrial College of the Armed Forces,National Defense University,Fort McNair,Washington,DC,20319-5062**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**28**	

INFORMATION & COMMUNICATIONS TECHNOLOGY 2007

ABSTRACT

The Information & Communications Technology (ICT) industry provides enabling capability for all major industries. The US ICT industry leads the world but must overcome several near-term challenges if it hopes to retain its global leadership. Some of the key challenges include reforming H1-B visa allocations to maintain a strong US-based IT workforce, monitoring the on-going convergence of telephony, data, and video services, resolving the debate over Internet neutrality, and supporting the full implementation of the National Critical Infrastructure Protection Plan. This research paper suggests roles for the global community, the US government and US business to address these and other concerns. Lastly, a growing industry constituency is fostering a paradigm shift to a Service Oriented Architecture (SOA) which fundamentally alters delivery of ICT capability to end users.

ICT Seminar Members
William Adamson, COL, US Army
Raji Bezwada, Defense Contract Management Agency
David Doe, Lt Col, US Air Force
Jeanette Duncan, Department of the Army
Akhil Govil, Defense Threat Reduction Agency
Timothy Harms, Department of Energy
Luwanda Jones, COL, US Army
James Karnes, Department of Defense
Felipe Morales, Lt Col, US Air Force (ANG)
John Morrison, COL, US Army
David Opatz, CDR, US Navy
Phil Pratzner, Lt Col, US Air Force
John Scorsone, Col, US Air Force
Victor Sparrow, Office of the Secretary of Defense
Robert Thomas, Department of the Army

Faculty
Richard Altieri, COL, US Army (retired)
Ken Alford, COL, US Army
David King, Colonel, Canadian Forces (retired)
Dr. Lynne Thompson, Col, US Air Force (retired)

FIRMS, AGENCIES AND ORGANIZATIONS VISITED:

Local Visits and Speakers:
Comcast Corporation
IBM Federal Systems, a division of IBM
ICSA Labs, a division of Cybertrust, Inc., Mechanicsburg, PA
Information Technology Association of America, Rosslyn, VA
National Cable and Telecommunications Association (NCTA), Washington, DC
National Telecommunications & Information Administration (NTIA), Washington, DC
Northrop-Grumman, Northrop Grumman Information Technology, Rosslyn, VA
Nortel Government Solutions, a division of Nortel Networks Ltd, Fairfax, VA
Office of Management and Budget, Washington, DC
Software and Information Industry Association (SIIA), Washington, DC
Telecommunications Industry Association
The Information Technology and Innovation Foundation
Verizon Communications
Vonage Holdings Corporation

Domestic Field Study:
Apple, Inc., Cupertino, CA
Brocade Communications Systems, Inc., San Jose, CA
Cisco Systems, Inc., San Jose, CA
Google, Mountain View, CA
Oracle Corporation, Redwood Shores, CA
Sun Microsystems, Inc., Santa Clara, CA

International Field Study:
American Institute in Taiwan (AIT), Taipei, Taiwan
American Chamber of Commerce in Taipei, Taiwan
Industrial Technology Research Institute (ITRI), Taiwan
Taiwan Semiconductor Industry Association (TSIA)
Chunghwa Telecom, Taiwan
Taiwan FarEasTone, Taiwan
BenQ Corp., Taiwan
American Chamber of Commerce, Japan, ICT Committee, Tokyo, Japan
Asian Technology Information Program (ATIP), Tokyo, Japan
NTT DoCoMo, Tokyo, Japan
US Embassy, Tokyo, Japan
BDA (China) Ltd., Beijing, China
Nortel China, Beijing, China
Microsoft Research Advance Technology Center, Beijing, China
US Information Technology Office (USITO), Beijing, China
Google, Beijing, China

INTRODUCTION

Information and Communications Technology (ICT) has changed the way in which business is conducted world-wide, thus creating a truly global information-centric world. ICT is also drawing the world together, in a cross-border flow of trade, investment, finance, information technology, culture, values, ideas and people regardless of their location in the world. It is enabling decisions, events, and people everywhere in the world—no matter how distant—to influence safety, prosperity, and policies (The Global Century, 2001, p. XIII). Finally, ICT continues to significantly influence world economies, world socio-cultures, and global governance, politics and policies. This dynamic industry's impact on the world over the last fifteen years is undeniable. Still, this industry has many challenges and only appropriate public policy that ensures its health and continued growth will enable it to continue its positive and lasting impact.

This paper examines this remarkable industry. First, it defines the industry. Second, it analyzes the current industry conditions. Third, it assesses the ICT industry's primary challenges. Fourth, given the current conditions and challenges, this paper projects an industry outlook in both the short and long term. Fifth, it proposes appropriate goals and roles of the United States government. Sixth and last, it takes a closer look at the major issues transforming the industry today. Although this industry is never stagnant, it does contain some basic elements, which uniquely define it, and will most likely be evident for many years to come.

THE ICT INDUSTRY DEFINED

ICT is an all-encompassing term that combines the terms/concepts of information technology (IT) and electronic communications. As defined by the Organisation for Economic Co-operation and Development, ICT contains "those industries which facilitate, by electronic means, the processing, transmission and display of information." (OECD-DSTI, 2005, p. 101). In broad terms, the ICT industry incorporates both manufacturing and services relating to information technology and telecommunications (OECD Glossary, 2006, par. 1). In determining the types of firms that constitute the industry, the study drew on the U.S. Census Bureau Economic Census data, the Securities and Exchange Commission EDGAR system, and the various ICT industry public policy organizations.

The ICT industry contains four major categories: hardware (computer, video, audio and network), software, information services and communications. More specifically, the ICT industry consists of following sectors: cable, telephone, television and radio manufacturing, cellular phones, software, computer hardware, network hardware, the Internet, data storage and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. All of these sectors have been significant and synergistic players in the rise of globalization.

INDUSTRY CURRENT CONDITIONS

Three conditions are particularly noteworthy in examining this industry. First, ICT has enabled growth globally. Second, and closely related, ICT has had a "flattening" effect, enabling countries to compete globally for ICT related work. Third, ICT has had a significant social impact throughout the world, and especially in the US. Taken together, these conditions convey that ICT is making a significant global impact.

Global Assessment

The Global Information Technology Report (GITR) 2006-2007 is the world's "most respected assessment of the impact of information and communication technology (ICT) on development processes and the competitiveness of nations". The report identifies ICT as a critical enabler impacting the world economy, "ICT is … an essential instrument for countries … to ensure continued prosperity for their people." The Networked Readiness Index (NRI) used in the report measures the propensity of countries to employ ICT for development and increased competitiveness and establishes an international framework for mapping out the enabling factors of such capacity" (World Economic Forum, 2007,).

The NRI uses three main component indices: environment, readiness and usage. These indices provide insight on a "country's current ICT infrastructure, investment climate and regulatory environment,…, the size of the human resource pool …, and the utilization of ICT in everyday life, etc" (Goswami, 2006, p. 1).

Networked Readiness Index Variation 2006-2007

Countries	Score 2006	Rank 2006-2007	Rank 2005-2006	Evolution	
Denmark	5.71	**1**	3	↗	+2
Sweden	5.66	**2**	8	↗	+6
Singapore	5.6	**3**	2	↘	-1
Finland	5.59	**4**	5	↗	+1
Switzerland	5.58	**5**	9	↗	+4
Netherlands	5.54	**6**	12	↗	+6
United States	5.54	**7**	1	↘	-6
Iceland	5.5	**8**	4	↘	-4
United Kingdom	5.45	**9**	10	↗	+1
Norway	5.42	**10**	13	↗	+3
Canada	5.35	**11**	6	↘	-5
Hong Kong SAR	5.35	**12**	11	↘	-1
Taiwan, China	5.28	**13**	7	↘	-6
Japan	5.27	**14**	16	↗	+2
Australia	5.24	**15**	15	→	0
Germany	5.22	**16**	17	↗	+1
Austria	5.17	**17**	18	↗	+1
Israel	5.14	**18**	19	↗	+1
Korea, Rep.	5.14	**19**	14	↘	-5
Estonia	5.02	**20**	23	↗	+3

Table I. Networked Readiness Index (Dutta, 2007, p. xix)

The GITR assessed 122 economies all over the world, which is double the number of countries assessed in 2000 (Dutta, 2007, p. x). Although the US arguably led the ICT revolution, ICT has rapidly become critical to every successful economy. According to the report, the United States dropped from the top position to seventh position. Table I below depicts the top twenty ranked countries. According to the 2006 Information Technology Outlook, world ICT spending has increased 5.6% yearly over 2000-05 in current US dollars, which is enabling the emergence of new growth economies. Internet-related investments and portable/consumer applications were identified as very dynamic segments of the ICT market, with the major share of venture capital continuing to flow into ICT (Information Technology Outlook 2006 Highlights, 2007, p. 3).

ICT's "Flattening" Effect

Like venture capitalists, individuals have also benefited from this industry. The decline in the cost of ICT technology has provided underdeveloped countries in Asia, Africa, and Latin America the tools to be competitive in many markets. People in these countries are using the World Wide Web for a multitude of tasks relating to their livelihood, for example, weather and crop price information or verifying village land-ownership from government websites (Bidgoli, 2006, p. 18). Whether used for personal survival or professional gain, ICT has "flattened the playing field," providing powerful tools for individuals in any country to engage, participate and compete globally in political, social and economic terms.

The Social Impact of ICT

These very same US firms and consumers have been transformed over the last 15 years by ICT. In 1992, a university senior in the US could see little difference between the world they were entering as working adults compared to the world that their parents entered decades earlier. A decade and a half later, the US has seen significant ICT penetration —computers, the Internet, broadband and wireless devices are common everywhere — and they have driven spectacular changes, in the workplace and in social networks (See Figure 1).

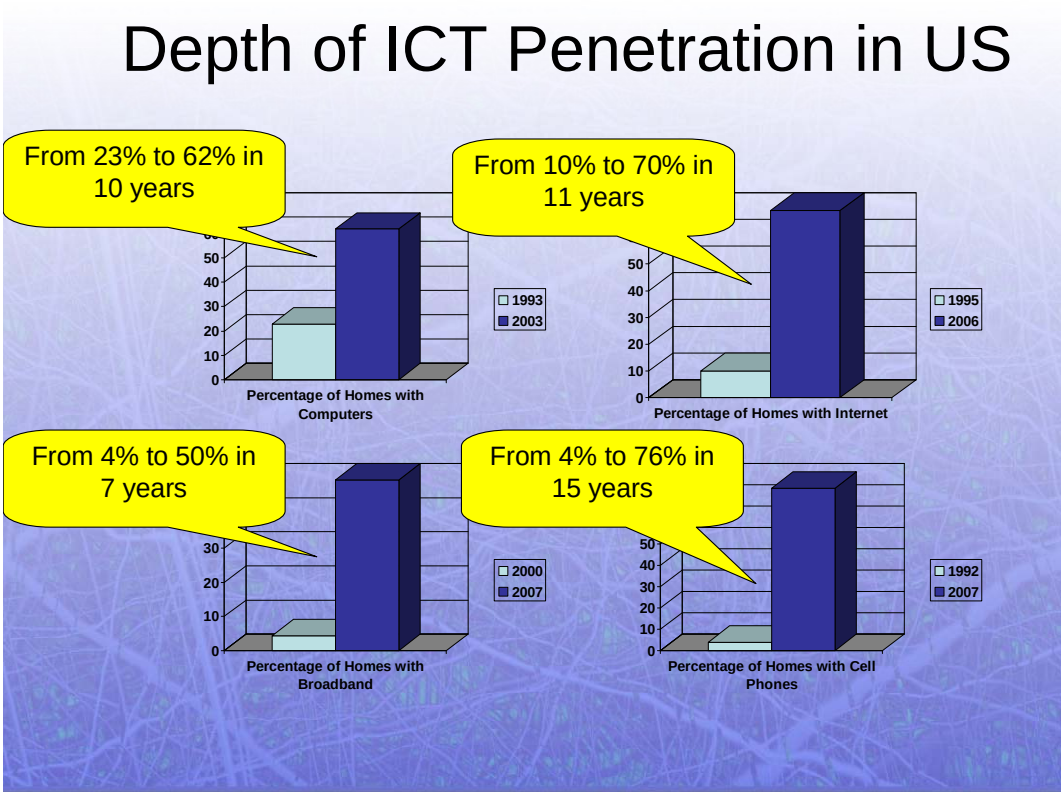

Figure 1. Depth of ICT Penetration in US (Day, 2005, p.1, Internet World Stats, CTIA, NTIA)

ICT is revolutionizing the way Americans work and interact socially. Today's American youth, who have never lived without computers or cell phones, will further steer both workplace and social network norms into uncharted territory. Two noteworthy trends are apparent from this penetration. First, networking, especially among youth, has grown dramatically, impacting the

way Americans obtain news and socially interact with each other. People can now interact and maintain contact with both friends and those they have never met through social networking sites such as MySpace.

Second, collaboration is now often the way work gets done—and this collaboration knows no distance, nor borders, nor rest. Work gets done on the same project sequentially around the clock in the US, India and China. These two trends have resulted in substantially more teleworking in the last fifteen years and differences in the way companies interact with their employees as well as relationships developed over the Internet. Communities of interest of every type and kind — teenagers, terrorists, faith-based organizations, hobbyists — have all found ways to connect and collaborate through ICT-enabled tools.

In short, while the world remains largely bifurcated in terms of ICT, the initial digital divide introduced by the Internet is beginning to breakdown.

ICT TRENDS AND CHALLENGES IN THE US

Workforce

US productivity and competitiveness in the ICT industry depends on several factors: first, the competence of its domestic ICT workforce, in terms of education and training; second, immigration policy in dealing with foreign workers to address domestic labor shortages; and third, offshore outsourcing as a means to remain competitive. ICT is rapidly changing, requiring both workers and companies to remain ever flexible in developing new skills. Additionally, the increased use of ICT by business coincides with demands for new and different job skills (Digital Economy, 2003). The US workforce must deal with all these challenges to remain competitive on a global scale.

Competence of Domestic Workforce. The Technology CEO Council, an advocacy group that includes leaders from Dell, EMC, Hewlett-Packard, IBM, Intel, and Sun Microsystems, stated that the more talented technical people the US can develop and attract to this country, the better for the economy and the nation. (Galvin, 2006). There is a perceived need within the industry, and perhaps the polity at large, to develop a homegrown ICT labor force, not only for the viability of the economy and the industry, but also for national security requirements. However, with unemployment among professionals at an inflation generating level of less than 2% (BLS, April 2007 data), substantial economic tradeoffs are implied. Nevertheless, the American Competitiveness Initiative (ACI) addresses many of these issues, ranging from education to employee training, and commits $5.9 billion in FY 07 to support these efforts (Domestic Policy Council, 2006, pp. 1-2).

Recruitment & Visas. While the US is struggling with producing domestic ICT talent, many other countries are producing an oversupply. The explosive growth of higher education in many developing countries, particularly in Asia, has caused a shift in the global talent pool. China and India are producing more engineers than all industrial countries combined. Other industrialized countries are aggressively recruiting from these countries. Meanwhile, the US has erected barriers for skilled migrants by restricting non-immigrant H1-B professional worker visas after 9/11. Additionally, enrollment of foreign students in US higher education declined for the first time since the 1950s as a result of Congress restricting F-4 student visas. This aversion towards foreign workers is depriving US universities and businesses of the talent necessary to drive American innovation. If these skilled individuals cannot enter the US market, more firms will be driven to offshore outsourcing.

Offshore Outsourcing. US worker productivity, for both intellectual and manual labor, no

longer exceeds foreign worker productivity for many of the countries previously mentioned. At the same time, two-thirds of the economic benefit from outsourcing accrues in the United States in the form of lower prices, expanded overseas markets for US products, and improved profits that are reinvested to create new jobs (McKinsey, 2003). These two dynamics provide ample incentives for companies to outsource offshore. Although beneficial in many ways, offshore outsourcing creates uncertainty (and, perhaps some degree of social and political instability) among domestic workers.

Recommendations

- Implement the initiatives relating to education in the ACI: "*Strengthens* K-12 math and science education by enhancing our understanding of how students learn and applying that knowledge to train highly qualified teachers, develop effective curricular materials, and improve student learning" (Domestic Policy Council, 2006, p. 3).
- Implement the initiatives relating to employee training in the ACI: "*Reforms* the workforce training system to offer training opportunities to some 800,000" (Domestic Policy Council, 2006, p. 3).
- Increase the number of H1-B and education visas to pre-9/11 levels.

Net Neutrality

Net Neutrality is one of the most discussed items in the industry, impacting a vast array of ICT firms. Exactly what is it? Net Neutrality is centrally linked to the idea that "broadband service providers charge consumers only once for Internet access, do not favor one content provider over another, and do not charge content providers for sending information over broadband lines to end users" (Hahn & Wallsten, 2006, p. 1). It is actually a benign-sounding name for price regulation:

> Influential coalitions of economic interests and academics have proposed that local broadband Internet access providers be prohibited from restricting access to their systems by upstream suppliers of Internet services. Much of the academic interest in net neutrality arises from the belief that the open architecture of the Internet under current standards has been responsible for its remarkable success, and wish to preserve this openness (Owen & Rosston, 2003, p. 1).

What does it mean to the average American? Today, Google, Amazon, and Microsoft want government to regulate Internet access prices at zero in the name of "net neutrality." Whereas

> …broadband Internet providers like Verizon, AT&T, and Comcast want to try charging content providers like Google for sending information to consumers over their lines. Such regulation could substantially reduce investment incentives, distort innovation, and ultimately harm consumers (Hahn & Wallsten, 2006, p. 1).

In considering the reasons to regulate the Internet, this paper asserts that regulation should only be passed when it benefits the majority and enables innovation. Legislation in support of Net Neutrality could be beneficial using this litmus test. "Identifying potential uses for the Internet and developing the corresponding applications is the prerequisite for realizing the enormous growth potential inherent in the Internet as a general-purpose technology" (van Schewick, 2005, p. 37). But there is also the risk that passing legislation on Net Neutrality may not be beneficial and have an adverse impact on growth and innovation in this market. Investors will not take risks in markets where the government directs policies such as those currently placed on the wired lines of the telecommunications market, as they discourage infrastructure improvements.

Given this dilemma, will Congress pass this piece of legislation? It is doubtful that the 110th Congress will take on such a controversial topic prior the next Presidential election. It is also generally thought that anti-trust laws will sufficiently allow the government to prevent monopolistic behavior. In general, the Internet should continue to be neutral. The success of Net Neutrality has been proven over the past several decades. A neutral Internet provides the greatest degree of content at the lowest price to consumers and fosters innovation and creativity within this powerful medium. Lastly, in order for regulation to be effective there must be a mechanism for enforcement and to measure performance. If you can't enforce it, you can't regulate it.

Recommendations

- Refrain from regulating, but ensure the Internet remains neutral to foster creativity, innovation, and the greatest degree of content at the lowest prices to consumers.
- When necessary, utilize existing anti-trust law to prevent monopolistic behavior.

Threats Arising from Developments in ICT

Although the benefits of advances in ICT are overwhelmingly positive, several potential dangers also exist. The number of cyber-attacks is increasing everyday. People want to know their personal data and privacy will be protected. Recently, there have been numerous headlines depicting network intrusions where confidential data such as social security numbers, credit card numbers and expirations, and home addresses, was potentially compromised. Growing dependence on ICT for key functions such as operating critical infrastructures creates vulnerability to attacks against this "cyber Achilles' heel." Additionally, the pervasiveness of networked information systems in more aspects of our private and professional lives increases the risk that personal information may be compromised. The US can ill afford to let up its guard when it comes to protecting its networks and personal data.

Critical Infrastructure Protection. ICT critical infrastructure is essential to the US economy and is vital to the continuity of operation of federal, state and local governments. Defining and rapidly implementing measures to protect the ICT critical infrastructure must be a high priority effort for the government, the private sector and the citizens of the United States. A partnership between the federal government and technical representatives from the telecommunications sector is essential to ensuring continuity of operations and continuity of government. The answer to ICT critical infrastructure protection is not one which should rely only on government regulation. The US has made strides recently in protecting critical infrastructure through publication of the National Infrastructure Protection Plan in 2006. The plan establishes a coordinated approach to protect critical infrastructure and key resources (NIIP, 2006).

Use of the model represented by the North American Electric Reliability Corporation of collaboration between the private sector and the government should be explored and expanded – nationally and even internationally. Work should be done to identify and implement redundant server networks and other methods of minimizing the potential of single point failures. Telecommunications, the Internet and related ICT industries have proven to be integral to the daily lives of United States citizens. Therefore, it is imperative that important aspects of the industry be considered critical infrastructure and protected. The need for cyber-security is increasingly central to the well-being of all US governments and their citizens.

Data Mining. An example of how important access and exploitation of data is to our economy today is evident in the practice of data mining. Data mining is the extraction of new and useful information from large amounts of data. The estimated amount of digital data

generated in 2006 was 161 billion gigabytes; it is expected to increase six-fold by 2010 (Gorman, 2007, p. 1). However, human analytic capacity has not kept pace. The gap between generation and analysis has created a "data-rich, information-poor environment," which some 60% of companies now tap into using data mining (Bannan, 2005, p. 35).

Firms mine data to identify those potential customers most likely to respond or convert from competitors, increase return on marketing costs investment (Harvey, 2006, pp. 37-38), and differentiate their services according to customer preferences rather than mass marketing. Other benefits include: market segmentation, reduced customer churn, fraud detection, interactive and direct marketing, and trend analysis.

Data mining, especially when conducted by government, involves six broad categories of risk (TAPAC, 2004, pp. 33-42): chilling effects (people behave differently when observed), aggregation (inequalities arising from data profiles), data processing (disclosure, retention, misuse and security), inaccuracy (decisions made with invalid information), false positives (mislabeling individuals as terrorists, tax cheats, etc.), and mission creep (data collected for one purpose, but later used for others). The U.S. has also found itself a target of adversary data mining enhanced by "electronic dissemination and search engines" (Bruce, 2003, p. 399).

Privacy with respect to data mining refers more to the intended use of information than to access (a security concern). To balance the costs and benefits, consumer/citizen choice is a key factor in data mining public policy. Effective *self-governance* depends upon a firm's integrity, and how well it establishes trust with its consumers. To this end, privacy policies should explain how data will be used, request consent, and allow consumers to opt in or out.

Recommendations

- Ensure the measures of the National Infrastructure Protection Plan are implemented.
- Refrain from regulating the commercial development or use of data mining technologies and applications—market forces should drive supply and demand.
- Enact comprehensive legislation regarding Federal collection, sharing, analysis and protection to US persons.
- Employ an interagency panel to develop supporting policies for data mining, paying special attention to national security needs and privacy protection.
- Government and industry should partner to improve capabilities in data mining and reduce the uncertainty inherent in correlative inferences.

GOVERNMENT GOALS AND ROLES

Government Regulation

The U.S. needs to conduct a thorough review of its current legislation and regulatory policy because rapid changes in technology and convergence in telecommunications has made many elements of regulatory control archaic. Overall, this paper provides very few recommendations for increased government intervention in ICT and advocates a light regulatory "footprint" on this industry. The following topics are some key areas in which government has intervened in this industry or may intervene in the future. Telecommunication convergence is not mentioned here but will be discussed in the Major Issues portion of the paper.

Universal Service. The Federal Communications Commission requires universal service "contributions" from telecommunications providers to subsidize basic phone service for low-income or rural providers, to subsidize high-cost phone companies, to provide reduced-price Internet service to schools and libraries, and to offer lower-priced telecommunications services to rural health care facilities (Ellig, 2006, p. 57). Overall, the Universal Service Fund is intended

to provide “parity among rural and urban consumers regarding access to telecommunications technologies and services” (Frieden, 2006, p. 11).

In 2004, the federal government spent $5.4 billion on these programs, with more $3.5 billion going to subsidize high-cost carriers (Ellig, 2006, p. 58). In other words, over half of the money in the Universal Service Fund is being directed to carriers that are not efficiently providing service. Universal service has been justified based on the assertion that telephone service is a “universal right” and that positive externalities result from having everyone connected to the telephone network. While this program transfers large amounts of money among different users, the extent to which they promote increased subscribership is unclear (Ellig, 2006, p. 60). Citizens living in rural areas, subsidized for years by other telephone users, now have a variety of ways to be connected to include wireless and satellite service.

ICT Research and Development Tax Credit. Most of the ICT industry associations visited by this study group strongly advocate for the permanent establishment of the R&D tax credit. However, there is not compelling evidence that a permanent R&D tax credit provides a significant boost to the ICT industry, especially when the cost of the tax credit is compared to the benefits to society as a whole. The ICT industry is already making substantial investments in the development of products which are demanded by industry and consumers. Overall, a permanent tax credit would impose a subsidy burden on of the rest of the economy.

Internet Governance. In the 1990s, **“**bottom-up” governance of the Internet was popularized by the “techno-libertarians” (Drake, 2004, p. 2). This group of programmers and academics believed that the Internet was mostly decentralized and virtually ungovernable. The primary arguments used by those favoring market-based governance are as follows: 1) “Bottom-up” governance of the Internet is fundamental to its creativity because ideas and innovations originate from a variety of people and institutions. 2) The “top-down” telephony model overseen by the International Telecommunication Union is inappropriate for the Internet because it would put policy in the hands of a central body along with national governments and stifle market-based innovation and pricing. 3) The current arrangement for establishing Internet standards by bodies such as the Internet Engineering Task Force (IETF) and Worldwide Web Consortium (W3C) is working well in that open standards and processes are leading to effective solutions.

However, countries and individuals are becoming increasingly concerned that a lack of “control” exists over the Internet. At one extreme of this argument are leaders in China, Iran, Burma, and Uzbekistan who censor Internet content in their countries. The leadership of these countries believes that the Internet should be administered by a U.N.-mandated treaty, which guarantees them the right to filter content coming into their countries. At the other end of the argument are those who appreciate the creative evolution of the Internet but are genuinely concerned about the lack of mechanisms in place to prevent hacking, spam, and cyber-crime.

The following are some of the main arguments used by those who contend a “top-down,” U.N.-like structure are needed to govern the Internet: 1) the United States government exerts too much control over the Internet through its quasi-official relationship with the Internet Corporation for Assigned Names and Numbers (ICANN). 2) The current arrangement over the “dot com” registry is monopolistic in that the private firm VeriSign has control over 75% of the domain name registrations through its relationship with ICANN (Business Week Online, 2006). 3) There is a lack of mechanisms to provide security, monitor spam, and prevent cyber-crime. In the future, this may cause people to seek safer, closed networks.

For the most part, “bottom-up” governance of the Internet is best. However, the proliferation of spam and crime on the Internet will need to be addressed by the governments of

countries across the world. Nations will have to cooperate and establish cross-border mechanisms, through organizations such as the Internet Governance Forum, to prosecute those who produce spam and viruses. The current arrangement is not effective and could lead to significant degradation of this ultimate "network of networks."

Government Involvement in Other Countries

The global ICT industry operates in a relatively unrestricted trade policy environment. The foreign companies and institutions that the seminar visited did not take issue with any particular trade restrictions. However, most countries, the US included, wield some degree of government influence over ICT firms' operations. The US employs foreign ownership restrictions in telecommunications (e.g. T-Mobile), restricts foreign ICT firms' participation in government contracts, and compels some services through regulation, e.g., rural telephones through the Universal Service Fund, as previously discussed.

In contrast to the private equity model prevalent in the US, other countries governments often maintain a controlling equity interest in ICT firms. Taiwan's principal telephone company, Chunghwa Telecom, has 35.4 percent government ownership (Chunghwa Telecom, 2007, p. 11). NTT DoCoMo, the principal mobile service provider in Japan, also has substantial government ownership. ICT firms in China are 65-70 percent government owned. Government involvement directly affects foreign direct investment capital flows and potentially management and capital effectiveness as well as increasing the barriers and risks for new firms.

However, the study group also observed that government ownership often permits more rapid technology deployment than may occur in the US. Taiwan illustrates this point well. The Taiwanese government created the Information Technology Research Institute (ITRI), a consortium of private firms and government researchers partnering together in an effort to develop innovative technologies in several industries, notably in ICT and the semiconductor industries. ITRI receives tax payer support through government funding for the specific purpose of conducting research which is then passed to Taiwanese firms for development and commercialization. The government has an active decision-making role in this research and development process. The ICT seminar concludes that this essentially results in government picking the "winners and losers." This practice creates barriers to entry for start-up firms that do not enjoy such a stakeholder relationship with government. Government involvement can provide an unfair advantage, restricting competition, which may not be good for the industry.

In China and Japan, in advanced wireless services and broadband, the ICT study group witnessed a mixed record of success with respect to government intervention. The seminar observed that Asian telecommunications firms adopted new standards more easily than their American counterparts, because government stakeholders generally ensure a "friendly" regulatory environment. In terms of wireless, China and Japan have a much higher percentage of cellular customers who demand and utilize a wider variety of services than their U.S. counterparts. Japan's NTT DoCoMo, which is government subsidized, already provides third generation (3G) wireless services to 72 percent of the subscribers, while in China, 3G services will be launched until 2009. Meanwhile, the United States just started auctioning spectrum for 3G in 2006. In terms of broadband, both China and Japan have already established more extensive infrastructure than the U.S. However, broadband is underutilized in these countries, and it is the opinion of this seminar, that government intervention has resulted in inefficiencies in the employment of capital. The U.S. model, whereby firms such as Verizon and AT&T, make capital investments in broadband results in more efficient use of resources.

Recommendations

- Eliminate the Universal Service Fund for telephony and Internet connection.
- Eliminate the R&D tax credit.
- In conjunction with other nations, prosecute those who produce spam and viruses and commit serious cyber-crime in order to prevent debilitation of the Internet.
- Maintain private control and ownership of the ICT industry in the United States—this industry study did not find compelling evidence that government intervention in ICT in Taiwan, Japan, and China results in enhanced welfare to consumers or producers, especially when compared to the costs and inefficiencies that were present.

OUTLOOK

National Security Resource Requirements

The events of September 11, 2001 directed a beacon of light on the tenuous thread of security we have in the United States. World financial markets were severely disrupted by the strikes on the World Trade Center. Response efforts were significantly hindered through lack of integration and the loss of key communication nodes,. To protect both commerce and the public, government has placed a well-deserved focus on identifying and protecting critical infrastructure – 85 percent of which is owned by the private sector.

The Internet has become the backbone of American business. If this essential tool were denied to the private sector for an extended period of time, the US economy would be severely damaged. The Internet, along with earlier versions of many software programs, was not designed with security in mind. Information technology security is still an immature science. The information technology security personnel are developing best practices each day. Any security strategy should account for people, processes, facilities, and technology. “Virtually all of the recent high-profile Internet attacks were successful because network managers continue to overlook simple security problems” (Tippett, 2002, p. 1 and 2). Dr. Tippett suggests five easy security actions to protect a network: turn off unneeded services in boxes attached to the Internet; never use a Web server for anything else; regularly apply security patches to critical machines; block all executable attachments at the gateway; use screen saver lockouts” (Tippett, 2002, p. 3).

The personal data of private citizens, as well as proprietary information resident in corporate databases, are constantly under threat of cyber-attack. Although data mining may be used to analyze and make decisions based on these types of data, it is generally employed for legitimate purposes. For example, the US government currently mines data for reasons ranging from improving its performance, to detecting fraudulent activities, to supporting law enforcement and intelligence (GAO, 2004, p. 8). Federal agencies pay as much as $50M per year for data on US and Latin American citizens, to conduct employee background checks, identify probable terrorists, and track border crossings (Swartz, 2003, p. 16). Besides contributing directly to economic growth, the $1.85B data mining industry (Donaldson, 2007, p. 96) is well-postured to meet US national security surge and mobilization requirements.

Increasingly, concerns with cyber-security compel firms to enact innovative security measures to combat cyber-attacks. “The law alone won’t prevent an unauthorized visit or even a deliberate attack” (Bono, Rubin, Stubblefield, and Green, 2006, p. 41). Many cyber-attacks occur from other countries and are difficult to trace and prosecute. “Security through legality is the misconception that an adversary will not pursue some avenue of attack just because doing so is unlawful…Criminals do not generally let laws stand in the way of breaking laws” (Bono, Rubin, Stubblefield, and Green, 2006, p. 42). It may be best to let market forces resolve how to address

cyber-security. Greg Garcia, the cyber-security czar for the Homeland Security Department, said that when customers or partners refuse to do business with companies that do not meet certain cyber standards, "that's when the groundswell for improving security is going to come" (Greenfield, 2006. p. 1).

Recommendations

- Continue government-industry work through the National Institute of Standards and Technology to develop the appropriate standards to protect networks and computers.
- Continue to work with the International community to address international cyber-crime and cyber-terrorism by creating treaties to work together to prosecute those who commit cyber-crime and cyber-terrorism from outside their borders.

Short and Long-term Outlook

The Way Forward. The ICT industry has transformed the way we work, shop and play. All industries now rely on the power derived from ICT and its services. The future is expected to bring an even greater proliferation of cell phones, high-speed, high-memory computers and broadband Internet access has provided innovative products that users never imagined possible. The list of potential emerging technologies over the next 10 years is nearly limitless.

Short-term Outlook. In the next 3 years, users will see an explosion of wireless broadband to mobile devices that will provide phone, Internet, MP3 players, Global Positioning System (GPS) mapping, video-on-demand downloads, live television, location-based information services, on-the-spot financial transactions and real-time mobile video-conferencing. Additionally, the exponential employment of radio frequency identification (RFID) + GPS location transmission devices will allow customers to track anything, anywhere, anytime.

Long-term Outlook. In the next 7 years, nanotechnology manufacturing will vastly increase the speed and memory capacity of computers. In the next 10 years, breakthroughs in quantum computing will allow computers to do pattern recognition and artificial intelligence processing that will likely exceed the ability of the human brain. The convenience of these new technologies also brings a new set of vulnerabilities. Currently, industry is spending the preponderance of R&D money on products that they can speed to market. The focus is on technology deliverables (the D of R&D) and not enough on the R. The federal government is not spending enough to make up for this industry shortfall. This lack of sufficient funds will make us vulnerable as a nation to security and economic threats. Accordingly, our recommendations are exclusively focused on the US government, and particularly the Department of Defense.

Recommendations

- Embrace the ICT industry's development activities for wireless broadband and RFID technology, quickly harvest more powerful mobile personal digital assistants (PDA) and fully employ RFID to improve supply chain management functions.
- Study new and innovative uses for mobile communications and RFID to solve additional national security problems.
- Seed selective (national security specific) research, but leave industry to continue to conduct the development work on nanotechnology.
- Take the lead and fund basic research initiatives with quantum computers given the Department of Energy and the National Security Agency needs for advancements in super computers.
- Remain vigilant to make appropriate policy adjustments given unforeseen breakthroughs in ICT.

One development which offers great promise to deliver quicker more effective ICT solutions in the future is Service Oriented Architecture (SOA). This paper contends that SOA is a fundamentally different, but more effective approach to government ICT challenges both now and in the future. Accordingly, this approach requires further explanation and development.

Service Oriented Architecture (SOA)

Historically, business and government enterprises purchase computer hardware, develop specific software applications to help manage their business processes, and hire a staff of IT professionals to maintain their IT systems and modernize IT infrastructure. This practice traditionally burdens the enterprise with IT life cycle replacement costs as technology advances and legacy systems become out-dated, isolates the enterprise's data from business partners or even from one department to another, and requires employees to be at their offices to access software applications and required data. This IT delivery model faces massive transformation with the advent of Service Oriented Architecture, or SOA.

The Delivery Model of the Future. SOA is a capability delivered to the consumer as ICT deployed as a hosted service and accessed over the Internet. SOA is a "game changer" approach for delivering ICT capability to business enterprises. SOA empowers information technology in the face of change to deploy solutions quicker. It ensures functions and data are integrated and is accessed collaboratively. The SOA vendor hosts critical applications and associated data on central servers at the vendor's location, and it supports the hardware and software with a dedicated support staff. This relieves the customer organization from the responsibility for supporting the hosted software, and for purchasing and maintaining server hardware for it. It is dependent on 'always on' web services where processes are separated from functions. It reduces redundancies and ensures interoperability and automated processes. It relies on both, governance and compliance as well as a mature, functional network infrastructure capable of reliably delivering these hosted services. It affects people, processes, platforms, and practices (Sun video notes, 2007).

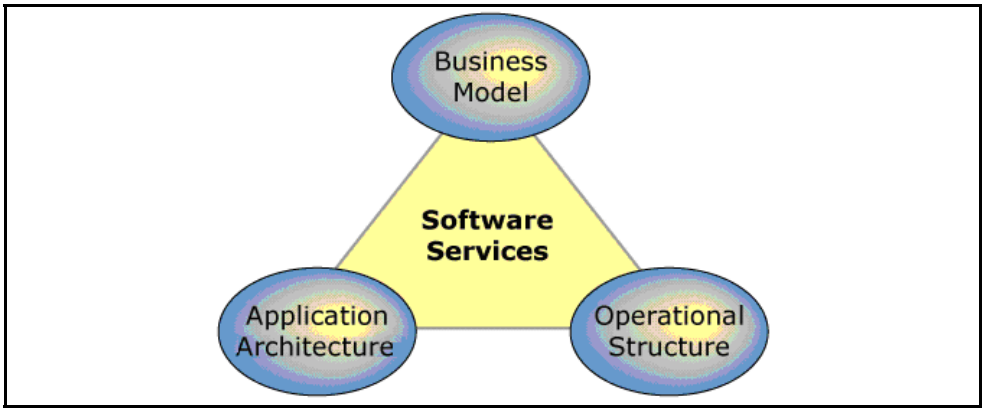

Figure 2. Software vendors need to shift their thinking. (Chong, 2006)

ICT organizations and businesses are managing complex ICT portfolios. Many of their critical business systems operate in isolation from other critical business systems—despite having business processes that span multiple applications. "To obtain an end-to-end view of a complex business process necessitates integration of information and process silos. In the past, this has been accomplished either though time-consuming manual interventions, or through hard-

coded solutions that are difficult to maintain" (Learn about Service Oriented Architectures, 2006, p. 1). However, today Service Oriented architecture is a strategy that "proclaims the intention to build all the software assets in the company using the service-oriented programming methodology" (CIO, 2007, p. 1). "Service Oriented Architecture is integrated software information and design approach that leverages Web computing standards for delivering business functions as shared services" (See Figure 2) (Sun video, 2007).

Service orientation is a way to organizing stove-piped systems/application into an integrated solution that breaks down stove-piped information and maximizes business agility. Service orientation modularizes IT resources by creating "loosely coupled business processes that integrate across business systems" (Learn about Service Oriented Architecture, 2006, p. 1). Business processes are critical service-oriented architecture because SOAs are creating business process solutions that are not constrained by the underlying IT infrastructure. SOA would not be possible without the Internet.

In ICT, the Future is Now. The objective for a SOA is accessing collaboration services that are published and available for use in a central repository, known as the Service Bus. Adopting SOA enables business agility and IT flexibility though the use of Web service protocols. According to Gartner & Associates, an ICT industry analyst company, "the majority of Fortune 500 companies will implement some type of SOA-based solution in 2007." SOAs require the implementation of a Service Oriented Environment that is based on the following principles:

- SOA is based on the "the policies, practices, and frameworks by which we ensure the right services are provided and consumed" (Learn about Service Oriented Architecture).
- With a SOA strategy, it is critical to implement processes that ensure that there are at least two different and separate processes — for provider and consumer.
- "Rather than leaving developers to discover individual services and put them into context, the Business Service Bus is instead their starting point that guides them to a coherent set that has been assembled for their domain." (Learn about Service Oriented Architectures)

> This is the beginning of the Business Web, argued Benioff, Salesforce.com's CEO, in a memo to his staff in November 2005. *The software industry is going through a transformation that is unlike anything it has seen in two decades, and comparable to the emergence of the PC itself…[italics added]* New Internet-based companies are showing how service will replace software for both consumers and corporations…Microsoft wants you to buy software. We want to see the end of software
>
> (Friedman, 2006, p. 89).

ESSAYS ON MAJOR ISSUES: ICT IS AN INDUSTRY IN TRANSFORMATION

Observation 1: Intellectual Property Rights (IPR) for Software

The development of software takes only intellect and time to produce. The main products of this industry are operating, utility, and applications programs. As the ICT industry grew in the 1980s, openness governed software development. As the ICT industry grew, consumers determined successful software applications through their purchasing power and software as a pre-packaged product became the industry standard. Intellectual property diffused as it entered the market as competitors entered the marketplace with imitations. Unlike most industries, the

source of “cost advantage”, the cost driver, became intellectual property (IP).

After software operates as designed its marginal cost approaches zero. The marginal cost of using the software, the cost of granting additional licenses is zero, or at any rate relatively small. The cost of developing a software program is unaffected by the extent to which its use is licensed. Distribution of software through the Internet further reduces cost and makes software ubiquitous. Open source software by definition is not marketable, because it can be uploaded for free.

> The genesis of the flat world platform not only enabled more people to author more content, and to collaborate on that content. …This newfound power of individuals and communities to send up, or out, and around their own products and ideas, often for free…is *fundamentally reshaping the flow of creativity, innovation, political mobilization, and information gathering and dissemination [italics added]*. Uploading is, without a doubt, becoming one of the most revolutionary forms of collaboration in the flat world.
>
> (Friedman, 2006, pp. 94-95).

Concern over trade secrets, piracy, and counterfeiting led to a proliferation of software patents beginning in the late 1980s. Conversely, as early as 1991, Bill Gates the founder of Microsoft stated, “If people understood how patents would be granted when most of today’s ideas were invented, and taken out patents, the industry would be at a complete standstill.” (Gates, 1991) Times have apparently changed. Microsoft, who estimated $14 billion in lost revenue to piracy in 2005, recognizes piracy in emerging markets can establish the company in a region and helps mitigate threats from free, open-source programs. Bill Gates, speaking at the University of Washington in 1998 stated, “As long as they're going to steal it [software], we want them to steal ours. They'll get sort of addicted, and then we'll somehow figure out how to collect sometime in the next decade…As economies mature and flourish and people and companies begin buying legitimate versions, they usually buy Microsoft because most others already use it. It's called the network effect” (Pillar, 2006). Microsoft’s acquiescence to piracy and willingness to suffer IPR infringement triggered a long-term strategy of consumer assimilation while expanding its market share.

Given the rate at which the ICT industry developed and continues to grow, 17-year monopoly rights inherit in a patent seem inordinately long and legally cumbersome to the future of the industry. Software copyright protection extends even further. The term for copyright protection encompasses “the life of an author plus seventy years or, if a corporation, ninety five years” (Lessig, 2001, p. 252). Finding a balance between these two divergent approaches: openness on the one hand, and monopoly rights on the other, represents the crux of the IPR divide within the ICT industry. A solution to the conflict between monopoly property rights and openness escapes easy resolution.

A novel delivery approach redefining how software enters the market called, Software-as-a-Service (SaaS), or software-plus-service, offers a promising alternative. SaaS, is distinguished from traditional pre-packaged, software, in that, SaaS represents a capability delivered to the consumer as "software deployed as a hosted service and accessed over the Internet" (Chong, 2006). The SaaS approach shifts “ownership” of software from the customer to an external provider. Instead of owning and installing a copy of software with its associated licensing agreement, a service is purchased on a subscription basis (Chong, 2006). With the SaaS delivery model, the software industry continues to innovate while regulating itself. Transforming the software industry to SaaS offers hope against piracy and fosters improved market efficiencies

and quality service. Google now offers office software applications following this model. As the shift to Service Oriented Architecture proliferates, and network infrastructure expands, this SaaS strategy will eventually reach consumers.

Recommendations

- Resist SaaS regulation if markets adequately regulate themselves
- Adopt the SaaS delivery model broadly across the US government as soon as the capacity of the network infrastructure allows.
- Monitor the progress made by industry with this delivery approach with additional research by future ICT seminars.

(COL Bill Adamson)

Observation 2: Convergence of ICT

Over the past few years, the unprecedented convergence of telephony, data, and video services, and the means by which these services are delivered, has begun to fundamentally alter the competitive nature of the telecommunications industry. The foundation of this revolutionary change is the industry's migration to a 'network of networks' based on an Internet Protocol (IP) architecture. As a result, consumers can now choose their telephony, video, and data services from among a variety of carriers. While network convergence is driving all aspects of the ICT industry, it is having a particularly profound impact on the ways that access to the "network of networks' is provided. For the first time, traditional cable TV and telephony companies that operated essentially as regional monopolies are now being forced to compete against each other; the deployment of new wireless and satellite services is further increasing competition in the marketplace. Convergence does pose certain challenges. It will significantly alter the telecommunications market and, in all likelihood, challenge the capacity of the Internet to support so many new services. Lastly, telecommunications convergence will force the US government to re-evaluate its current legislation and ensure that it is applicable to today's competitive environment. Telecommunications convergence is a reality, and its benefits and challenges will result in one thing for certain: increased competition—a benefit to consumers.

Convergence will challenge the capacity of the Internet on a global and local scale. Within the US, capacity is rapidly expanding due to a strong mix of public and private investment; however, carriers will face challenges meeting consumer demand to provide high bandwidth applications to 'the last mile.' Internationally, it is a different story, and "the unrelenting growth in Internet traffic [caused in part by convergence] may overwhelm….the terabit-capable pipes connecting the continents" (TMT, 2007, p. 6). The challenge remains that no single entity either monitors capacity or coordinates efforts to ensure that adequate backbone connectivity exists. In 2009, the U.S will release direct coordination control of ICANN to the global community. Acting as a 'watchdog' that assesses Internet backbone capacity and highlights potential shortfalls is a natural extension of the ICANN charter. The US should continue to rely on private investment based on standard technical underpinnings.

The convergence of information and communication technologies is enabling accelerated growth in the emergence of network dependent products and services. Voice over Internet Protocol, next generation technologies such as IPTV and IP multimedia subsystem will expand the need for more IP addresses.

Recommendations

- Adopt a 'light' regulatory touch that fosters competition at the local level and provides the consumer with choice.

- Ensure that the network remains open and that companies are not able to restrict the services or content that consumers wish to view or purchase.
- Maintain the ability of the consumer to choose services independently of 'bundled' packages in order to select the services that best meet their personal needs.
- Eliminate any remaining barriers to competition based off the 'regional monopoly' model for both the telecommunications and cable companies.
- Reduce infrastructure 'build-out requirements' and allow consumer demand to drive the installation of new infrastructure and the provisioning of new services.
- Eliminate rate regulation and franchise fees to foster new entrants to the marketplace; recent history demonstrates that service charges are either declining or, at minimum, remaining constant as new competitors enter the market.
- Eliminate any established performance standards that may neutralize product differentiation.

(COL John Morrison)

Observation 3: The Dawn of Internet Protocol version 6

Internet addresses needed for mobile devices and network dependent products are increasing as "voice, data and streaming video are starting to converge over IP networks" (Gartner, 2005, p.4). Mobile data devices are becoming accessible to more and more consumers at affordable prices which have the potential to drive the need for more IP addresses. "All computers across the Internet are assigned a unique identifier called an IP address. IP addresses are used like street addresses so other computers can locate them. IP addresses are numerical numbers between 0 and 255, separated by periods. For example, an IP Address may look something like: "56.234.22.12" (NovaWorks, 2003, par. 14).

Internet Protocol version 6 (IPv6) is the next generation Internet Protocol designed to replace the current version, Internet Protocol version 4 (IPv4), which is predominantly deployed throughout the United States. The rapidly growing Internet-based economy needs far more addresses than IPv4, with a 4.3 billion address maximum, allows. IPv6 provides trillions of new Internet addresses, enhances security and improves functionality. "We could allocate an IPv6 address to every grain of sand on all of the beaches on the earth and not come close to exhausting the range of possible addresses" (RAND, 2007, p. 56).

IPv6 ensures the successful implementation of DoD's Global Information Grid providing seamless communications, interconnectivity, and end-to-end set of information capabilities. IPv6 has the potential to enhance public safety, disaster recovery operations, and help support a "plug-and-play" environment. "In the future, IPv6 will allow vehicles to communicate with sensors in the road and with other vehicles to create smart lanes and avoid potential crashes. For example, if two vehicles get too close to each other, IPv6 technology will enable them to warn their drivers of the danger and begin applying the brakes automatically" (FCW, 2007, p. S8). IPv6 also promises to offer tighter security, known as IP Security (IPSec), to ensure authentication and encryption across the Internet which has the potential to facilitate more robust and secure e-commerce.

However, the deployment of IPv6 faces a number of challenges. In the United States, a majority of the Internet infrastructure is IPv4-compatible equipment. One of the biggest challenges converting to IPv6 is rewriting the decades old software and legacy programs to work with IPv6. Most of these programs were not written to be modular in nature, which leads to costly programming and testing. The implementation of IPv6 faces a number of additional challenges such as managing the dual existence of IPv4 and IPv6 environment during transition,

interoperability and security vulnerabilities. The Government Accountability Office report (2005) warns that if devices such as firewalls and intrusion-detection systems are not properly configured to accommodate IPv6 features, then IPv6 traffic may not be detected or controlled, leaving systems vulnerable to attack (p. 30). Federal agencies need to carefully evaluate these complexities as they proceed with the implementation.

Training is another aspect that is critical to this transformation. System engineers, network administrators, and designers must plan and choose the right diversified IPv6 ranges to ensure a smooth transition of networks from IPv4 to IPv6. Funding is crucial for transitioning to IPv6. However, the US can not afford to wait until the IPv4 and its associated systems slow the adoption of innovative applications and solutions. As mentioned earlier, IPv6 is a critical component of DoD's GIG interconnectivity concept of operations. IPv6 is essential to the continued growth of the Internet. It is also critical to meet the growing demands of mobile community.

In addition, the timing of IPv6 deployment may potentially raise broader strategic issues and technological challenges such as international competitiveness. There are concerns among key stakeholders that the United States is lagging behind in implementing IPv6. Many other countries including China, Taiwan, and Japan are ahead of the United States in adoption of IPv6. The cost of transformation may be an important factor, but not adopting IPv6 may jeopardize our nation's ability to maintain its competitive advantage.

Recommendations

- Assume a proactive government role to encourage IPv6 transition both within and outside of federal government.
- Require federal agencies to plan for an upgrade to the next-generation IP during their normal equipment upgrades. This will enforce the Federal Agencies to control costs and plan for IPv6 deployment.
- Partner government with industry to develop standards and transition plans. This initiative will help develop best practices, mitigate security risks, and take advantage of lessons learned to reduce overall costs, schedule delays and ensure a smooth transition.

(Raji Bezwada)

Observation 4: Radio Spectrum Management

The rapid growth of wireless subscriber services worldwide creates a large demand for radio spectrum. A host of factors propels this growth: the economy has moved towards the communications-intensive service sector, the workforce is increasingly mobile, and consumers have been quick to embrace the convenience and increased efficiency of the multitude of wireless devices available today. Consequently, commercial demand for wireless services has created a more competitive environment for radio spectrum.

However, many factors, from technical to regulatory, constrain the availability of radio spectrum for wireless services. Technical and regulatory innovation on both fronts should allow consumers to continue to experience new wireless services. Spectrum efficient technologies and regulatory reform should overcome what is, in essence, a *notional spectrum shortage*. Current policies regarding the radio spectrum do not take into account the time dimension of spectrum use. In addition, current policies do not allow new technologies to take advantage of geographic *white space*, or unused spectrum.

From a global perspective, the use of wireless infrastructure in lieu of wired infrastructures by emerging countries permits modernization at much lower cost. However,

emerging technologies, new applications, and wireless based services strain current spectrum management policies. But smart technologies, such as software defined radios (SDR), potentially allow operators to take advantage of the time dimension of the radio spectrum. Frequencies can be changed nearly instantaneously allowing use of allocated but unused spectrum. Cognitive radios, as well, would allow the sensing and acquisition of unused spectrum. These technologies are undoubtedly the wave of the future.

Recommendations

- Adopt regulations which allow dynamic access to the radio spectrum.
- Provide incentives for spectrum efficient technologies which will improve spectrum utilization.

(Vic Sparrow)

Observation 5: E-Commerce/Business

Electronic Commerce is the distributing, buying, selling, marketing and servicing of products or services over electronic systems such as the Internet. E-commerce can expand business and consumer access to markets and reduce production marketing costs. There are two major types of e-commerce: business-to-consumer (B2C) and business-to-business (B2B). B2C is where consumers purchase products and services from businesses.

In B2C, the Internet enables consumers to purchase an unprecedented array of goods and services from the convenience of their homes. Consumers can find and purchase thousands of goods, from thousands of suppliers from around the world, and have those goods delivered to their doors. In many instances, these consumers may find lower prices and a greater variety of goods and services online than in bricks-and-mortar stores. B2B is where businesses buy and sell among themselves. Retailers can reduce their purchasing expenses and enhance supply chain efficiencies by using business-to-business e-commerce (Shim, S., Pendyala, V., Sundaram, M., Gao, J. 2000 p. 40).

The Japanese mobile phone company NTT DoCoMo is providing a mobile e-wallet service. A chip on the back of a mobile phone can be used to move across a scanner to purchase tickets on the Tokyo Metro or at movie theatres. NTT is working on expanding the places the e-wallet can be used at retail stores and restaurants. The advantages of e-wallet are low transaction cost and convenience of not having to carry money or credit cards.

Two sub-components of e-commerce are e-banking and e-government. Electronic banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. The comprehensive features and functionality offered by e-banking enables a bank to reduce consumer cost and increase consumer benefit, at the same time improve efficiency, reduce the cost of operations, and generate revenues. Electronic government refers to government's use of information and communication technology platforms to exchange information and services with citizens, businesses, and other arms of government (OCED). E-governments provide an efficient and effective channel for governments to facilitate their internal administration and to improve their external services (Brewer, G., Neubauer, B., Geiselhart, K. 2006 p. 477).

The Federal and State governments currently regulate some aspects of e-commerce and will likely increase regulation in the future. E-banking, brokerage services, tele-medicine and tele-pharmacy industries are already regulated. Taxation, gambling, security and online privacy could soon be regulated by the government (Rayport, J. 2002 p. 597). Taxation is an issue because e-commerce companies do not have to collect sales tax on their customers' purchases. While this is an advantage to consumers, it costs state and local governments billions of dollars a

year in forgone tax revenues from traditional business operations. Gambling is an issue because the Internet makes it difficult to decide where the transaction takes place, and therefore, which region's law should regulate that transaction (Rayport, J., 2002 p. 597).

Recommendations

- Allow the market to regulate itself to help increase competition and foster innovation.
- Regulate only to obtain a comprehensive policy for security and online privacy.

(Jim Karnes)

CONCLUSION

The course of study through the spring 2007 semester revealed that the Information and Communications Technology industry has become "the game changer" industry for the world economy. The Internet has become the global backbone of world economies. Disruption of the network "backbone" negatively affects all industries and all countries. No industry can succeed in the global economy without ICT technologies and services. In fact, Friedman suggests the "world is flat" predominantly because of global advances in information technology. Three concerns dominate the evolution of the ICT industry within the US: potential deficiencies in the US ICT workforce, the unsettled controversy over net neutrality, and cyber-attacks against critical ICT infrastructure coupled with information assurance.

A preeminent issue for ICT firms visited by this seminar was access to talent and the limitations imposed by H1-B Visas for foreign workers. This study supports broadening the approval of H1-B Visas to pre-9/11 levels. The US economy benefits by permitting the entry of well-educated, foreign born ICT professionals. The alternative of not adjusting Visa levels risks US competitiveness in ICT by restricting a highly educated and skilled work force to other countries.

The highly contested debate between content providers and telecommunications companies over net neutrality puts at risk the current paradigm of unrestricted access to content over the Internet. This research forwards the position that access to information over the network should be provided much like a utility service. The expectation should be much like how electricity or water is delivered to the home. Flip the switch and turn on the faucet, and the lights should come on and the water should flow. Similarly, access to Internet content should be available at no additional cost, not tiered service with filtered content monitored and controlled by internet service providers (ISP), which because of their oligopoly, and in some cases monopoly, market power, may act to restrict access to content. ISP should simply provide the Internet pipes to consumers.

A new approach to ICT delivery promises to transform the industry with the advent of SOA. The SOA delivery model signals that the industry is ready to provide ICT capability to the end user as a service. This practice will relieve business enterprises of legacy equipment replacement costs and software application upgrades. The growth in the use of software-as-a-service demonstrates that SOA is becoming a reality. However, this paper reveals that an SOA approach is only possible if the network infrastructure remains reliable while additional high bandwidth requirements strain its capacity. Convergence of telephony, data, and video services creates even greater demands on infrastructure capacity. The network infrastructure will be further challenged as IPv6 increases the quantity of IP addresses needing high bandwidth access and E-commerce and E-business becomes the prevalent form of conducting business in the global economy.

This research paper suggests roles for the global community, the US government and US business to address the concerns noted previously. In sum, each has a vital role to play in ensuring the health and promoting the growth of this industry. US firms must work very closely with the US government—indeed, it is within their own self-interest to police each action, and ensure execution of these actions is within appropriate legal and ethical framework. They should also take steps on their own, both to benefit themselves and guarantee the health of the industry as a whole.

The unprecedented growth and rapid technological advances in ICT technology continue to outpace government regulation. For this reason, and the many others cited throughout this paper, this research concludes that the ICT market must be allowed to govern itself. This fosters the competitive atmosphere required to nurture further innovation in this industry ultimately benefiting the global market place.

References

Bannan, K. (2005, September). 12 tips for generating rich data. *Customer Relationship Management, 9*(9), 34.

BDA. (2007, May 9). *China's ICT market and service innovations*. Briefing presented at BDA, Beijing, China.

Bidgoli, H. (2006). *Handbook of information security: Key concepts, infrastructure, standards, and protocols*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Bono, S., Rubin, A., Stubblefield, A., & Green, M. (2006). Security through legality. *Communications of the ACM, 49*(26), 41-42.

Bound, J., & Junaid, I. (2006). *IPv6 application note: 3rd Generation WiFi - carrier class secure mobility*. IPv6 Forum.

Brewer, G., Neubauer, B., & Geiselhart, K. (2006). Designing and implementing e-government systems. *Administration and Society, 38*(4), 472-499.

Bruce, J. B. (2003). *Intelligence and the national security strategist: Enduring issues and challenges* (R. Z. George & R. D. Kline, ed.). Washington, DC: NDU Press.

Bush, G. W. (2003, February). *The National Strategy for The Physical Protection of critical infrastructures and key assets*. Retrieved April 3, 2007, from http://www.whitehouse.gov//physical_strategy.pdf

Bush, G. W. (2006, February 2). *American competitiveness initiative.* Retrieved May 14, 2007, from Domestic Policy Council, Office of Science of Technology Policy Web site: http://www.whitehouse.gov////

Business Week Online. (2006, June 19). Internet oversight: A crucial test. In *Viewpoint*. Retrieved March 5, 2007, from http://www.businessweek.com///

Chong, F., & Gianpaolo, C. (2006, April). *Architecture strategies for catching the long tail*. Retrieved April 2, 2007, from Microsoft Corporation Web site: http://msdn2.microsoft.com/us//.aspx

Chunghwa Telecomm. (2007, May 3). *Key challenges and strategies facing ICT industries*. Briefing presented at Chunghwa Telecomm, Taipei, Taiwan.

CIO Magazine. (2007). *An introduction to SOA.* Retrieved April 21, 2007, from http://www.cio.com//

Cooper, K. B., & Gallagher, M. D. (2004, September). *A Nation online: entering the broadband age*. Retrieved April 17, 2007, from National Technology Industrial Association Web site: http://www.ntia.doc.gov///.htm

CTIA. (n.d.). *Wireless Quick Facts*. Retrieved March 17, 2007, from The Wireless Association Web site: http://www.ctia.org//.cfm//0323

Day, J. C., Janus, A., & Davis, J. (2003). *Computer and Internet use in the United States*. Retrieved April 17, 2007, from U.S. Census Bureau Web site: http://www.census.gov// pubs/-208.pdf.

Department of Homeland Security. (2006, June 30). *National infrastructure protection plan*. Retrieved May 17, 2007, from http://www.dhs.gov///_Plan.pdf

Donaldson, S. A. (2007, March). Profiting from consumer behavior. *Black Enterprise, 37*(8), 94-97.

Drake, W. (2004, February). Reframing internet governance discourse: Fifteen baseline propositions. In *Workshop on Internet Governance*. Retrieved March 15, 2007, from http://www.ssrc.org////Drake2.pdf

Dutta, S. (2007, March 29). *Global information technology report 2006-2007: Executive summary*. Retrieved March 30, 2007, from http://www.weforum.org///.pdf

Ellig, J. (2006, January). Cost and consequences of federal telecommunications regulations. *Federal communications law journal, 58*(1), 37-102.

Federal Computer Week (FCW). (n.d.). Boost Your Car's IQ. In *Tech Watch IPv6*. Retrieved March 27, 2007, from http://www.fcw.com///.html

Federal Reserve Bank of San Francisco. (2005, October). *The rise and spread of R&D tax credits*. Retrieved May 15, 2007, from http://www.frbsf.org

Frieden, R. (2006). *Killing with kindness: Fatal flaws in the $5.7 billion universal service funding mission and what should be done to narrow the digital divide*. Retrieved March 10, 2007, from http://papers.ssrn.com//.cfm?abstract_id=762344

Friedman, T. L. (2005). *The world is flat: A brief history of the twenty-first century*. New York, USA: Farrar, Straus and Giroux.

Gartner. (2005, December). *U.S. Government's move to IPv6 will require disciplined implementation* (Rep. No. G00136319).

Gates, B. (1991, May 16). *Challenges and strategy*. Retrieved March 2, 2007, from http://www.bralyn.net///.gates/strategy.txt

Gorman, S. (2007, March 10). Chief of NSA urges 'action'. In *Baltimore Sun* (p. 1). Retrieved March 31, 2007, from http://www.balimoresun.com///te.nsa10mar10,1,340516.story?ctrack=1&cset=true

Goswami, D. (2006, September 16). *A Review of the network readiness index*. Retrieved May 16, 2007, from World Dialogue for Networked Economies Web site: http://www.regulateonline.org////

Government Accountability Office (GAO). (2004, May). *Data mining: Federal efforts cover a wide range of uses* (Rep. No. GAO-04-548). Washington, DC. Retrieved March 31, 2007, from http://www.gao.gov/.items/.pdf

Government Accountability Office (GAO). (2005). *Internet Protocol Version 6: Federal Agencies need to plan for transition and manage security risks* (Rep. No. GAO-05-845T). Retrieved March 22, 2007, from http://www.usipv6.com/sense///%20-%20Powner%20IPv6%20Testimony.pdf

Greenfield, H. (2007). *Panelists struggle to find answers to cyber threats*. Retrieved March 17, 2007, from National Journal's Technology Daily Web site: http://www.govexec.com/// tdpm2.htm.

Harvey, P. (2006, August). Data mining in the 21st century. *Target Marketing, 29*(8), 37-39.

Institute for National Strategic Studies, National Defense University (Producer). (2001). *The Global century: Globalization and national security* [Motion picture]. USA: National Defense University Press.

International Telecommunication Union (ITU). (2007, February 7). *7th Global Symposium for Regulators: Delivering real benefits to industry and customers including costs reduction and innovative new services*. Retrieved March 29, 2007, from http://www.itu.int//_releases//.htmlhttp://

Lessig, L. (2001). *The future of ideas*. New York, USA: Random House.

Microsoft Corporation. (n.d.). *Service oriented architecture*. Retrieved April 21, 2007, from http://msdn2.microsoft.com/us//.aspx

Microsoft Corporation. (2006). *Learn about service oriented architecture*. Retrieved April 22, 2007, from http://www.microsoft.com////.mspx

Miniwatts Marketing Group. (n.d.). *Internet world stats*. Retrieved April 11, 2007, from http://www.internetworldstats.com//.htm

Miniwatts Marketing Group. (n.d.). *Internet world stats*. Retrieved April 11, 2007, from http://www.internetworldstats.com//.htm

NovaWorks. (2003). IP address. In *Domain Names Glossary* (par. 14). Retrieved April 2, 2007, from http://www.domain-name-center.com/name-glossary.htm

NTT DoCoMo. (2007, May 7). *NTT DoCoMo overview*. Briefing presented at NTT DoCoMo, Tokyo, Japan.

Organisation for Economic Co-operation and Development (OECD). (2005). *Annex 1B: OECD definition of the ICT sector*. Retrieved May 14, 2007, from http://www.oecd.org////.pdf

Organisation for Economic Co-operation and Development (OECD). (2006). Information, communication technology (ICT) sector. In *Glossary of statistical terms*. Retrieved May 15, 2007, from http://stats.oecd.org//.asp?ID=3038

Organisation for Economic Co-operation and Development (OECD). (2007). *Information technology outlook 2006 highlights*. Retrieved March 30, 2007, from http://www.oecd.org////.pdf

Organisation for Economic Co-operation and Development (OECD). (2007, May 14). *OCED E Government Projects*. Retrieved May 16, 2007, from http://webdomino1.oecd.org///.nsf

Pendyala, S. S., Sundaram, V., & Gao, M. (2000). Business-to-business e-commerce frameworks. *Computer, 33*(10), 40.

Pillar, C. (2006, April 18). How Microsoft benefits from rampant piracy. In *LA Times*. Retrieved April 6, 2007, from http://www.macdailynews.com/.php///_microsoft_ben

RAND. (2007). *Security challenges to the use and deployment of disruptive technologies.*

Rayport, F. J. (2002). *Introduction to e-ecommerce*. Boston: McGraw-Hill/.

Schewick, V. (2005, September). Towards an economic framework for network neutrality regulation. In *The 33rd research conference on communications, information and Internet policy*. Retrieved March 10, 2007, from The National Center for Technology and Law, George Mason University School of Law, Arlington, VA, USA Web site: from http://web.si.umich.edu//// /%20Schewick%20Network%20Neutrality%20TPRC%202005.pdf

Sun Microsystems. (n.d.). *Discover service oriented architecture*. Retrieved April 21, 2007, from http://www.sun.com////_soa/.html?intcmp=75

Swartz, N. (2003, July/). U.S. data-mining spurs investigations in Latin America. *Information Management Journal, 37*(4), 16.

Technology, Media & Telecommunication (TMT). (2007). Technology Predictions 2007. Retrieved April 1, 2007, from http://www.deloitte.com/dtt/cda/doc/content/dtt_TelecomPredictions011107.pdf

Technology and Privacy Advisory Committee (TAPAC). (2004, March). *Safeguarding privacy in the fight against terrorism*. Retrieved March 31, 2007, from Department of Defense Web site: http://www.cdt.org///tapac.pdf

The Wall Street Journal. (2007, May 2). U.S. Fed chief decries trade curbs. *The Wall Street Journal*, p. 3.

Tippett, P. S. (2002). *Keep It Simple: Making your enterprise more secure with less effort*. Herndon, VA: TruSecure, Inc.

U.S. Census Bureau. (1998, March). *Census brief* (Rep. No. CENBR/-2). U.S. Census Bureau. Retrieved April 17, 2007, from http://www.census.gov//pubs/.pdf.

World Economic Forum. (2007, March 28). *Denmark climbs to the top in the rankings of the world economic forum's global information technology report 2006-2007*. Retrieved May 16, 2007, from http://www.weforum.org///%20Press%20Releases/_2007_press_release

World Information Technology and Services Alliance (WITSA). (n.d.). Executive summary. In *Digital planet 2006*. Retrieved April 25, 2007, from http://www.witsa.org// /_ExecSummary.pdf